人工智能技术在核设施实物保护系统网络安全检测中的应用

王赛

（国家核安保技术中心，北京 100000）

摘 要：随着时代的发展与进步，我国核设施面临的网络安全防护形势非常严峻。在网络安全防护中合理运用人工智能技术，可以增强网络安全防护的针对性，更好地保障网络系统的安全稳定运行。本文以相关理论为基础，探讨了人工智能防御网络攻击关键技术，提出了人工智能在核设施实物保护系统网络安全检测中的应用策略，旨在利用人工智能技术精准检系统存在的网络安全隐患，提升核设施实物保护系统网络安全检测的实时监测、智能分析、自动化响能力，有效抵御外部的病毒和攻击，提高系统网络的安全性和稳定性，切实保障核设施实物保护系统的网络和数据安全。

关键词：人工智能技术；核设施实物保护系统系统；网络安全检测；网络和数据安全

Application of Artificial Intelligence Technology in Network Security Detection of the Nuclear Facilities Physical Protection System

Wang Sai

(Center of Excellence on Nuclear Security, Bejing 100000,China)

Abstract:With the development and progress of the times, the cybersecurity protection situation faced by nuclear facilities in China is extremely severe. The rational application of artificial intelligence (AI) technology in cybersecurity protection can enhance the pertinence of cybersecurity protection and better ensure the safe and stable operation of network systems. Based on relevant theories, this paper explores the key AI technologies for defending against cyberattacks, and proposes application strategies for AI in the cybersecurity detection of nuclear facility physical protection systems. The aim is to use AI technology to accurately detect potential cybersecurity risks in the system, improve the real-time monitoring, intelligent analysis, and automated response capabilities of cybersecurity detection in nuclear facility physical protection systems, effectively resist external viruses and attacks, enhance the security and stability of the system network, and effectively safeguard the network and data security of nuclear facility physical protection systems.

Keywords：artificial intelligence technology；Nuclear Facility Physical Protection System；network security detection；artificial intelligence algorithm；Network and Data Security

0 引言

近年来，随着网络化、信息化以及数字化时代的到来，互联网网络规模持续扩大，已日渐成为我国通信网络核心基础设施，在民生、经济、交通运输等领域发挥重要作用，极大地提升了工业生产的自动化能力，为人们的生活带来了诸多便利。与此同时，黑客技术、网络恶意攻击等行为呈现出智能化、多元化发展趋势，传统网络安全检测技术难以精准识别新型攻击手段，面临着检测准确率低、行为特征提取困难等问题。在此背景下，将人工智能技术引入网络安全检测领域，丰富检测手段、强化检测模型泛化能力，全面检测系统中存在的网络安全漏洞，针对的制定防护方案是打造安全网络环境的重要前提。

实物保护系统是保障核设施安全，确保核材料一克不丢一克不少的关键基础。随着自动化、信息化技术的不断发展，核设施实物保护系统也越来越依赖于网络技术和信息系统。然

而，这也使得系统面临着来自网络的各种威胁，如黑客攻击、病毒传播等。因此，提升核设施实物保护系统网络安全检测能力，消除系统中存在的网络安全隐患，确保核设施实物保护系统的网络安全，对于保障核设施安全稳定运行具有重要意义。

1 网络安全威胁概述

网络安全威胁是指任何可能对网络系统的机密性、完整性、可用性造成损害的因素或行为。这些威胁可能来自内部或外部，包括恶意攻击、非授权访问、数据泄露等，最终造成用户信息泄密、计算机系统崩溃等后果。目前，网络安全隐患呈现出多样化发展趋势，攻击手段持续更新，常见网络攻击方式包括恶意软件、服务器访问攻击、跨站请求伪造、跨站脚本攻击、暴力破解等[1]。从网络安全检测角度来看，网络攻击行为更新速度超出安全检测技术发展步伐，传统安全检测手段很难精准识别到新型攻击行为，致使网络环境实质上存在安全漏洞，无法彻底解决各项网络安全问题。人工智能具有认知能力、学习能力、自动化能力以及决策能力等，其与网络安全检测技术的发展与融合应用，对精准识别系统中存在的网络安全隐患，针对性的制定解决方案，进一步提升系统网络安全具有重要意义。

2 核设施实物保护系统网络安全概述

核设施实物保护是指防止核材料被盗和非法转移、防止核设施被破坏而采取的一系列保护措施和技术。核设施实物保护系统是采用探测、延迟及响应的技术和能力，阻止破坏核设施的行为，防止盗窃、抢劫或非法转移核材料活动的一个综合性安全防范系统。包括视频监控系统、出入口控制系统、入侵探测报警系统以及集成管理系统等技防措施，保卫人员、公安武警等人防措施，以及实体屏障等物防措施。随着信息化、数字化技术的不断发展，核设施实物保护系统越来越依赖于网络技术和信息系统。因此，系统同样也面临着各种各样的网络安全威胁，主要包括：

1) 外部网络攻击：黑客可能通过网络攻击手段，试图入侵核设施实物保护系统，窃取敏感信息或破坏系统正常运行。

2) 恶意软件感染：病毒、蠕虫等恶意软件可能通过网络传播到核设施实物保护系统中，对系统造成损害或窃取关键数据。

3) 数据泄露风险：系统中存储的大量敏感数据，若被泄露，将对核设施的安全构成严重威胁。

4) 内部人员威胁：内部员工可能因各种原因（如恶意行为、疏忽大意、误操作等）对系统造成威胁，如泄露密码、篡改数据等。

3 核设施实物保护系统网络安全检测的现状

首先，法规标准方面。国际上美国核管会等不断评估和修改法规，国际原子能机构也在完善相关标准和导则，但仍存在部分法规无法及时适用于新堆型首堆等问题。其次，检测方法方面。目前主要依赖传统的网络安全检测方法，如网络配置检测、安全漏洞扫描、恶意代码检测、网络流量监测和安全访问控制等，通过人工或自动化工具对网络设备、操作系统、应用程序等进行定期检查和评估。再次，安全挑战方面。随着核设施数字化程度提高，面临的网络攻击风险增加，如震网病毒对伊朗核设施的攻击。同时，核设施的复杂性和特殊性，

使得网络安全检测需考虑物理安全与网络安全的融合，以及内部知情人可能带来的更大威胁等问题。

4 人工智能算法概述

人工智能算法是模拟人类思维方式，代为执行各项决策任务的一项技术手段。在网络安全检测领域，无需用户全程监控网络环境，根据实时数据，从中提取网络攻击特征值，精准识别到当前存在的网络安全隐患。人工智能算法种类众多，主要分为专家系统、机器学习、神经网络三种类型，算法原理和网络安全检测手段有着本质不同。其中，专家系统由知识库和专家推理机制组成，全面收集网络安全事件案例，从中总结网络安全领域权威专家的专业知识，以及面向特定网络安全问题的通用解决方法，从网络数据内提取、对比安全隐患特征值，判定网络安全隐患性质，同步向用户提供处理建议。机器学习通过模仿人类行为方式，不断导入网络安全事件案例进行训练，根据预设规则来判定安全隐患类型，对比验证判断结果与实际结果，持续改进诊断规则[2]。神经网络同样通过模仿人类行为特征的方法来处理问题，具备分布式并行处理条件，由大量节点构建层次化网络结构，各处节点依次执行加权、求和、激活函数等数据处理任务，神经网络输出结果即为网络安全检测结论。引入人工智能算法后的变化。

（1）检测效率显著提升。人工智能算法能够快速处理大量的网络安全数据，如实时监测网络流量、系统日志等，快速识别异常行为和潜在的安全威胁，大大缩短了检测时间，提高了检测效率。如通过机器学习算法对历史数据的学习和分析，可以快速发现新的攻击模式和异常情况。

（2）检测精度大幅提高。利用深度学习等人工智能技术，可以对核设施实物保护系统中的各种数据进行深度挖掘和分析，提高对安全威胁的识别精度。通过对视频监控数据的智能分析，可以更准确地识别出可疑人员和异常行为，减少误报和漏报率。

（3）智能化预警与响应。人工智能算法可以根据检测到的安全威胁，自动进行预警和响应。例如，当检测到网络攻击或异常行为时，系统可以自动发出警报，并采取相应的措施，如切断网络连接、启动应急响应程序等，提高了核设施的安全性和应急响应能力。

（4）安全态势感知增强。通过对核设施实物保护系统的全方位监测和数据分析，人工智能算法可以实时掌握系统的安全态势，预测潜在的安全风险，为核设施的安全管理提供决策支持。例如，通过对网络流量、系统性能等数据的分析，可以预测系统是否存在安全隐患，提前采取措施进行防范。

5 人工智能防御网络攻击关键技术

5.1 基于人工智能的访问控制技术

非法访问控制是不法分子通过伪造 IP 地址等手段，伪装用户身份，非法访问计算机网络系统，获取用户操作权限，展开一系列破坏网络环境与实现非法牟利目标的操作行为，包括篡改文件内容、篡改系统设置、植入计算机病毒。在传统网络安全检测体系，主要通过账

户密码认证等落后手段来识别用户身份，很难精准验证用户真实身份。对此，需要依托人工智能算法，重新构建访问控制机制，以生物特征识别、行为习惯作为验证用户身份与访问控制的重要手段。

对于生物特征识别手段，提前构建生物特征数据库，存储用户生物特征信息，如面部信息、指纹信息以及虹膜信息，建立基于生物特征识别手段的网络系统访问控制流程，如图 1 所示。用户访问计算机网络系统时，通过配套装置，实时采集生物特征信息，智能算法负责分析采集信息和库内信息的相似度，确定相似度超过标准值后，方可确定用户真实身份[3]。对于行为习惯验证手段，持续跟踪监控用户操作过程，绘制用户画像，总结用户行为习惯，以及不同场景下最有可能采取的操作行为。用户通过验证，顺利访问计算机网络系统后，继续监控操作过程，如果本次操作过程和历史行为习惯相互冲突，或是操作行为连续多次有违智能算法预测结果，表明用户身份存疑，采取二次验证手段。

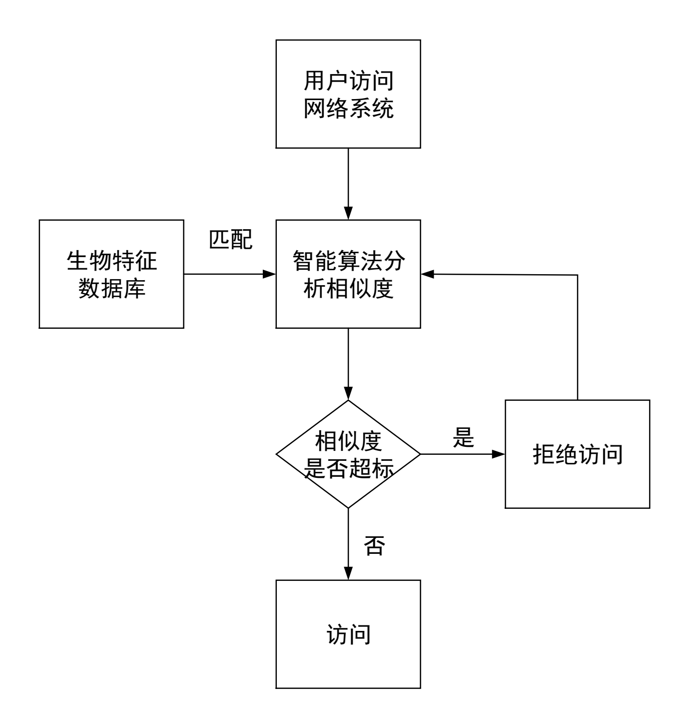


图 1 基于生物特征识别手段的网络系统访问控制流程

Fig.1 Network system access control process based on biometric identification means

5.2 利用强化学习智能体优化防火墙策略

防火墙作为网络安全防御体系中的一道重要安全防线，部署在内部网络与外部公共网络交界处，负责识别用户身份和拦截携带计算机病毒的数据文件。传统防火墙技术具备频繁报警询问的局限性，全部进程访问网络都向用户询问是否放行，这无疑会影响用户体验，同时，还要求用户具备一定的专业水平，如果用户无法自行判断网络安全隐患，也会导致计算机网络系统遭受恶意攻击。

针对以上问题，需要把传统防火墙技术和人工智能技术进行融合处理，构建新一代智能防火墙，依托人工智能算法来识别判定正常程序与含有病毒程序，无需请求用户协助。简单来讲，智能防火墙本身具备自我学习能力，自主学习网络流量模式，动态调整访问控制策略，持续健全、优化改进防火墙规则，科学制定面向不同类型网络攻击行为的防御方案，而不再

是机械性执行先期制定的安全策略。根据实践应用情况来看，在计算机网络系统，智能防火墙可以自行拦截恶意数据流量攻击、黑客攻击、IP 欺骗等网络攻击手段，并通过擦洗通信协议来消除潜在协议风险[4]。

5.3 自动化修复网络漏洞系统

应用人工智能技术，建立自动化漏洞扫描修复机制，从根源上解决问题。自动化漏洞扫描修复机制由漏洞知识库、智能扫描引擎、验证工具、修复工具链等部分组成，所构建漏洞知识库负责持续采集存储结构化漏洞信息，根据漏洞信息来生成扫描策略，交由智能扫描引擎执行，搭配使用到验证工具，精准找出网络安全漏洞分布位置，溯源分析漏洞形成过程，最终根据漏洞类型、特征，利用修复工具链，自行修复网络安全漏洞。人工智能技术落地应用期间，为改善漏洞修复效率与提高修复速度，应掌握多引擎协同智能扫描、数据流分析验证两方面的应用要点。

第一，多引擎协同智能扫描。基于插件化设计理念来构建扫描引擎调度框架，根据所处网络环境与知识库提供建议，组合使用多款引擎，共同执行扫描策略。扫描期间发现各处网络安全漏洞时，动态增加或是移除相关引擎，彻底解决单一引擎通用性差、环境适应能力不足的技术难题。第二，数据流分析验证。以污点分析作为漏洞验证手段，持续性追踪检测外部输入数据流向过程，提前定义污点源规则，模拟数据流转路径，根据数据流向判定是否触及漏洞点，统计污点传播路径和漏洞点交集情况，以此来验证网络安全漏洞是否真实存在[5]。

5.4 人工智能安全分析师与自动响应

在传统网络安全检测体系，本身缺乏安全隐患处理能力，仅能机械性被动执行先期设定的安全策略，在外部数据流入和计算机网络系统运行期间，找出各处网络安全隐患与扫描安全漏洞，把安全检测报告提供给用户，人工处理安全问题。安全隐患处理效果主要取决于用户自身具备的网络安全知识技能，如果用户本身缺乏相应技能，或是出现错误决策问题，无疑会导致网络安全问题长期存在，造成更为严重的损失。因此，需要应用人工智能技术来强化网络安全处置能力，整合安全检测、安全处理、安全态势评估在内的多项活动，共同构建功能齐全的网络安全防御体系。从实操角度来看，具体应用到人工智能安全分析师技术，以实现自动响应能力作为技术应用目标，确定计算机网络系统存在安全漏洞，以及遭受恶意攻击后，迅速评估安全威胁程度与感知安全态势，模拟权威专家人工决策过程，自行生成并执行应急处置决策，包括调整防火墙、隔离受损主机等，争取在最短时间内消除网络安全隐患、减轻网络系统总体受损程度。

6 人工智能在核设施实物保护系统网络安全检测中的应用

6.1 基于机器学习的入侵检测系统

在计算机网络系统入侵检测环节，可以采取机器学习类型的人工智能算法，组合采取监督学习方式与无监督自主学习方式。提前收集各类型网络安全事件案例，对历史数据进行标注处理，提交给机器学习算法进行训练学习，逐步掌握正常流量、异常流量识别方式和特征，训练后的机器学习算法即为初始检测模型。进入无监督自主学习阶段，持续把实时网络数据提交给智能算法，不断学习了解全新流量模式，确保智能算法足以适应动态变化的网络环境，

精准识别、应对新型攻击手段。为提高入侵检测精度，应掌握特征工程、纵深防御两方面的应用要点。第一，特征工程。多维度识别提取入侵特征，涉及到网络流量时间序列、负载内容以及协议行为等维度，并根据网络攻击类型来动态调整网络流量特征提取内容[6]。第二，纵深防御。组合应用人工智能和其他网络安全检测技术，构建纵深防御体系。智能算法识别到入侵行为后，信息反馈给防火墙、入侵检测等网络安全设备，同步调整防火墙、入侵检测等网络安全设备的防御策略，提升系统的防御能力。

6.2 利用深度学习模型检测恶意软件

恶意软件检测是网络安全检测流程中的一道重要步骤，推荐采取卷积神经网络算法，把恶意代码视作一类特殊图像，扫描滑动窗口，从中提取足够数量的局部特征，再把局部特征进行抽象处理后，精准刻画恶意代码整体模式[7]。也可选择采取循环神经网络算法，重点处理序列化数据，掌握学习序列内部依存关系，捕捉恶意行为时序特征。如果对检测精度提出严格要求，则组合采取两种人工智能算法，融合处理不同智能算法的输出结果，综合判定恶意软件。也可选择同时构建 TextCNN 分类模型和 XGBoost 模型，共同执行恶意软件检测任务，检测流程如图 2 所示。TextCNN 模型作为基于深度学习的分类模型，有着文本数据处理效率高、具备自学习条件的优势，特征输入值加入增加长距离 n 元组。XBGoost 模型以短距离 N-Gram 信息与整体语义信息作为特征输入内容，可以非线性表达联众信息，检测速度相对较快。TextCNN 分类模型和 XGBoost 模型的结合，能够在恶意软件检测任务中实现优势互补，提升检测准确率、效率、泛化能力和可解释性，为网络安全防护提供更强大的技术支持[8]。

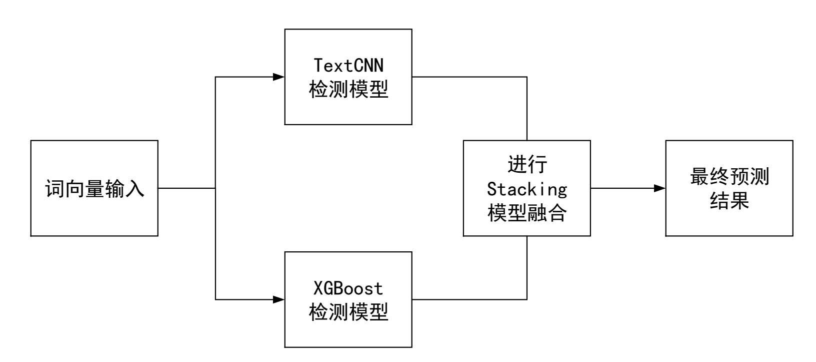


图 2 基于 TextCNN 分类模型和 XGBoost 模型的恶意软件检测流程

Fig.2 Malware detection process based on TextCNN classification model and XGBoost model

6.3 利用自然语言处理分析网络流量

网络流量分析环节，以自然语言处理作为分析手段，把网络负载数据本身含有的词语及字符串映射至低维空间，基于向量距离及相似程度来精准描述语义关系，从中判别恶意负载、私密信息泄露在内的网络安全事件。同时，在网络流量内提取包括 IP 地址、文件名在内的实体信息，把实体信息导入实体关联网络，根据分析结果来呈现攻击链条关系，进而推断恶意攻击行为主体、客体以及地点等要素信息，精准呈现恶意攻击过程全貌[9]。例如，在流量分类环节，自然语言处理技术负责标记不同类型数据，便于后续执行数据过滤、分类和处理任务，可分为正常数据、敏感数据以及恶意数据，分类独立处理不同数据。

6.4 通过大数据分析提高安全可视性

人工智能技术应用期间，网络安全检测系统的自动化水平有所提升，可以替代人工精准识别网络安全隐患与采取处置措施，但在遇到严重安全隐患时，仍旧需要人工介入。因此，提高安全检测结果可视化程度，成为网络安全检测体系有待完善的主要短板。组合应用人工智能技术与大数据分析技术，以精准识别安全隐患、可视化呈现网络安全态势作为功能定位。大数据技术负责高效处理多源异构数据，统一数据格式和去除无效数据后，把有效数据提交给智能算法进行处理，再把算法输出结果通过直观生动方式进行可视化呈现。例如，构建属性图模型，灵活表示复杂安全事件要素组成和关联情况，便于用户准确了解网络安全态势，采取最佳解决措施。

6.5 核设施实物保护系统网络安全检测与人工智能技术的结合应用

我国早期建设的核设施实物保护系统设备以国外产品为主，网络安全防御以物理隔离为主，侧重于计算机终端安全与数据安全的防护。新建的核设施实物保护系统设置物理隔离的同时也部署了防火墙、入侵检测系统、安全审计等基本的网络安全技术防护措施。常规的网络安全检测手段无法精准有效发现核设施实物保护系统中存在的网络安全风险和隐患，一旦不法分子突破物理隔离，挖掘利用核设施实物保护系统中存在的漏洞隐患，入侵、攻击系统会引起一系列网络安全事件，造成系统瘫痪、核心数据泄露，甚至会对核设施安全产生破坏。为精准识别实物保护系统中存在的网络安全风险和隐患，持续挖掘系统中存在的漏洞，应充分利用人工智能技术的优势，将其与核设施实物保护系统网络安全检测相结合，构建基于机器学习的入侵检测系统、利用深度学习模型检测恶意软件、利用自然语言处理分析网络流量以及通过大数据分析提高安全可视性的新型网络安全解决方案[10]。提升核设施实物保护系统网络安全检测的自主性、动态性、可视性以及决策性能力，达到不法分子“进不来、拿不走、看不懂、改不了、走不脱”的目的。真正做到及时发现威胁，及时分析威胁，及时制定解决方案，切实提升核设施实物保护系统网络安全能力。

7 结论

综上所述，为强化核设施实物保护系统网络安全防御能力，及时精确检测网络安全隐患，预防网络安全事件发生。应提高人工智能技术在核设施实物保护系统网络安全检测中的应用力度，全方位重塑网络安全检测体系，丰富检测手段、提高检测精度，重点强化入侵检测能力、恶意软件检测能力、网络流量分析能力和安全可视化能力，为核设施实物保护系统网络安全防御提供全新方法。通过实时监测、智能分析、自动化响应等措施，可以有效防范网络攻击和潜在威胁。未来，随着人工智能技术的不断发展和完善，其在核设施实物保护系统网络安全检测中的应用将更加广泛和深入，在保障核设施网络安全中发挥更加重要的作用。

参考文献

[1]程银龙.基于分布式人工智能的网络安全监测关键技术研究[D].哈尔滨工程大学,2022.

[2]钟再淳.基于人工智能的网络入侵检测与防御技术[J].网络安全技术与应用,2024,(12):6-8.

[3]郝春亮,张骁,王秉政,等.生物特征识别信息保护标准实施应用[J].信息技术与标准化,2022,(05):37-40+58.

[4]张凯俊.人工智能在网络安全威胁检测与预防中的应用[J].软件,2024,45(09):151-153.

[5]樊华.人工智能技术在大数据网络安全防御中的应用[J].中国高新科技,2023,(21):50-52.
[6]王冬梅.人工智能技术在网络安全威胁检测与防御中的应用研究[J].信息与电脑(理论版),2024,36(13):123-125.
[7]梅彬.基于人工智能理论的网络安全管理关键技术研究[J].信息网络安全,2021,(S1):66-69.
[8]李红.基于大数据技术的网络信息传输安全监测方法[J].网络安全和信息化,2025,(01):122-124.
[9]李丹.防火墙技术在网络信息安全监测中的应用研究[J].信息记录材料,2024,25(12):83-85.
[10]江海.基于人工智能技术的信息安全态势感知系统设计与实现[J].电脑编程技巧与维护,2024,(11):144-146.